IN THE SPECIFICATION:

Please amend the paragraph beginning on page 6, line 25, as follows:

The present invention may also be used to transmit data from the server 20 to the client 18 via the Internet 12. For example, the string generator 84 may be used to randomly generate and store a character string 116 in the database 100. The hashing engine 86 may hash the private key 110 corresponding to the client 18 with the character string 116 to generate the hash key 118. Using the hash key 118, the engine 88 may be used to encrypt data to be transmitted to the client 18. The encrypted data and the character string 116 are then transmitted from the server 20 to the client 18 via the Internet 12. The client 18 may then decrypt the data using the character string 116 and the private key 62 similar to as described above in connection with the server 20. For example, the hashing engine 42 may be used to hash the character string 116 generated by the generator 84 with the private key 62 to generate the hash key 64 for decrypting the received encrypted data 112. The signature engine 90 may also be used to generate a signature 120 corresponding to the transmitted data by hashing the hash key 118 with the data similar to as described above in connection with the client 18. The signature 120 may then be transmitted to the client 18 via the Internet 12. The client ~~118~~ 18 may then compare the signature 120 to a signature generated by the signature generator 46 using the hash key 64 and the decrypted data. The processors 30 and 80 may also be configured to incorporate a sequence number or identifier into the data 70 and 114 such that duplicate or out-of-sequence data transmissions received by either the client 18 or server 20 are discarded or rejected.